STORAGE MEDIUM RENTAL SYSTEM

This application is a Continuation-In-Part of Application Serial No. 10/234,093, filed on September 5, 2002, which is still pending.

Technical Field

The present invention relates to a technique for renting a storage medium storing digital content.

Background Art

Storage mediums such as DVDs for digitally storing work including movies and music have been increasingly widespread. High-volume information can be digitally stored in such storage mediums as DVDs, and can be used semi-permanently.

By taking advantage of such storage mediums, a rental-service business for renting storage mediums storing movies, music, etc., has been developed to create a huge market.

Japanese Laid-open Patent Application No. H11-164238 discloses the following technique, aiming at billing users economically in accordance with playback conditions of work. At a rental shop, a user selects, from a group of discs, a disc storing information that the user wants. At the rental shop, information about the selected disc, such as a serial number, a catalogue number, a specified playback time, and a playback number (=0), is written to an IC card owned by the user. The user plays the disc using a player to play back

the information stored therein. Here, a playback time is measured and accumulated. When the accumulated playback time exceeds the specified playback time, the playback number, which is the number of times the disc is played, is counted as one. The user may play the disc a plural number of times, and the counted playback number is written to the IC card. When the user returns the disc and the IC card, data in the IC card is read and an amount of payment is calculated in accordance with the playback number at the rental shop.

Also, Japanese Laid-open Patent Application No. H11-167768 discloses the following technique, aiming at managing a rental time limit, so that a rented disc can be played only within a rental-use period for the disc. At a rental shop, a user selects, from a number of discs, a disc storing software information that the user wants. Each disc also stores its unique management information. Information about the selected disc, i.e., unique management information and rental-use time limit information of the selected disc, is written to an IC card by an IC card writing apparatus. Then, the user is given this IC card together with the selected disc. The user brings home the disc and the IC card, and sets them on a special player. The player can play the disc only within the rental-use period that is written in the IC card.

Moreover, Japanese Laid-open Patent Application No. 2002-50126 discloses the following technique, aiming at

providing, at low costs, a playback apparatus that prevents playback of a storage medium whose rental time limit is expired, a storage medium, and a rental system. A data playback apparatus is equipped with a data playback control unit. The data playback control unit starts clocking time with an initial value being the start date and time of a playback-allowed period shown by management information. The playback-allowed period is a time period during which data is allowed to be played back. The data playback control unit allows the data to be played back until the kept date and time reaches the end date and time of the playback-allowed period. The rental system of this invention includes a data writing apparatus that writes, to a storage medium, data and its management information showing a playback-allowed period during which the data is allowed to be played back, the storage medium storing the data and the management information, and the above-described data playback apparatus.

Further, Japanese Laid-open Patent Application No. 2002-149061 discloses the following technique, aiming at providing a distribution system and a distribution method that improve user convenience, eliminate profit loss of a shop, and realize secure content protection in the field of digital content distribution. Mutual authentication is performed between a playback apparatus and an IC card and also between the IC card and a management center. The IC card

transmits, to the management center, a certificate of a playback apparatus public key that has been received from the playback apparatus. A user inputs, using a terminal, contract information including a content title and a rental period. The management center receives the contract information to which a signature of the IC card is added, encrypts a content encryption key and the like using the playback apparatus public key and the like, adds a signature to the encrypted data, and transmits the data with the signature to the terminal. The terminal writes the transmitted data to the IC card. When the signature matching succeeds, the terminal stores the content into the storage medium. The playback apparatus decrypts the encrypted content encryption key received from the IC card, and decrypts the content using the content encryption key.

There are increasing demands from rental agents that rent storage mediums storing movies, music, etc. for effectively limiting users' use of work stored in such storage mediums.

Disclosure of the Invention

To satisfy the above-mentioned demands, the present invention aims at providing a rental system, a playback apparatus, a rental-shop apparatus, a rental method, a storage medium, and a rental program that can limit a user's use of

a storage medium storing digital work when the storage medium is rented to the user.

In a storage-medium rental system, a rental agent rents a user a storage medium storing digital work, to provide the digital work to the user. The system includes a portable storage medium to be rented to the user, a portable semiconductor memory owned by the user, a rental-shop apparatus owned by the rental agent, and a playback apparatus owned by the user. The storage medium prestores encrypted content generated by encrypting digital work using a content encryption key. The semiconductor memory has an area for securely storing a content decryption key. The rental-shop apparatus stores a content decryption key for decrypting the encrypted content. When the user rents the storage medium at a rental shop, the semiconductor memory is mounted on the rental-shop apparatus. When the rental agent receives a user's payment for the rental, the rental-shop apparatus writes the content decryption key to the semiconductor memory. To play back the digital work, the user mounts the semiconductor memory and the storage medium on the playback apparatus. The playback apparatus securely reads the content decryption key from the semiconductor memory, reads the encrypted content from the storage medium, decrypts the encrypted content using the content decryption key, and play back the decrypted content.

The above aim of the present invention can be achieved by a storage-medium rental system for temporarily providing, from a rental agent to a user, a right to use digital work stored in a portable storage medium, where a portable semiconductor memory is connected to a rental-shop apparatus when the rental agent rents the user the storage medium, and the storage medium and the semiconductor memory are connected to a playback apparatus when the user plays back the digital work, the storage-medium rental system including: the storage medium that prestores digital content data representing the digital work; the semiconductor memory that has an area for securely storing information; the rental-shop apparatus that securely writes right information into the area of the semiconductor memory when the rental agent rents the user the storage medium, the right information showing a range of the right to use the digital work stored in the storage medium; the playback apparatus that, upon receipt of an instruction from the user to play back the digital work, (a) securely reads the right information from the area of the semiconductor memory, (b) judges whether the digital work is allowed to be used or not, based on the read right information, and (c) only when judging that the digital work is allowed to be used, reads the digital content data from the storage medium and plays back the digital work based on the read digital content data.

According to this construction, the rental-shop apparatus securely writes the right information to the semiconductor memory, and the playback apparatus securely reads the right information from the semiconductor memory and judges whether the digital work stored in the storage medium is allowed to be used or not based on the read right information. Therefore, only the user who owns the semiconductor memory can play back the digital work.

Here, the user may make a payment for rental to the rental agent when the rental agent rents the user the storage medium, and the rental-shop apparatus may securely write the right information into the area of the semiconductor memory when the rental agent receives the payment for rental from the user.

According to this construction, the rental-shop apparatus securely writes the right information to the semiconductor memory when the rental agent receives the payment for rental from the user. Therefore, the semiconductor memory can be used to guarantee that the user has properly made the payment for rental to the rental agent.

Here, the digital content data stored in the storage medium may have been generated by encrypting the digital work using an encryption key, the rental-shop apparatus may write the right information including a decryption key to be used to decrypt the digital content data, into the area of the

semiconductor memory, and the playback apparatus may decrypt the read digital content data using the decryption key included in the read right information, to generate the digital work, only when judging that the digital work is allowed to be used.

According to this construction, the playback apparatus decrypts the read digital content data using the decryption key included in the read right information. Therefore, only the user who owns the semiconductor memory can decrypt the digital content data.

Here, the rental-shop apparatus may securely write the right information including playback-limiting information into the area of the semiconductor memory, the playback-limiting information showing a limitation to be imposed on playback of the digital work stored in the storage medium, and the playback apparatus may judge whether the digital work is allowed to be used or not, based on the playback-limiting information included in the read right information.

According to this construction, the playback apparatus judges whether the digital work is allowed to be used or not, based on the playback-limiting information included in the right information read from the semiconductor memory. This construction can properly limit the use of the digital work by the user who owns the semiconductor memory.

Here, the playback-limiting information may show a

rental-use time limit until when the rental agent allows the user to use the digital work stored in the storage medium, the rental-shop apparatus may write the right information including the rental-use time limit, and the playback apparatus may compare the rental-use time limit included in the right information with a present date and time, and judges that the digital work is allowed to be used when the rental-use time limit is on or after the present date and time.

According to this construction, a rental-use time limit can be set for the user who owns the semiconductor memory.

Here, the playback-limiting information may show a rental-use period during which the rental agent allows the user to use the digital work stored in the storage medium, the rental-use period starting from a time at which the user firstly plays back the digital work stored in the storage medium, the rental-shop apparatus may write the right information including the rental-use period, and the playback apparatus may compare an elapsed date and time at which the rental-use period elapses from the time at which the user firstly plays back the digital work, with a present date and time, and judges that the digital work is allowed to be used when the elapsed date and time is on or after the present date and time.

According to this construction, a rental-use period can be set for the user who owns the semiconductor memory.

Here, the playback-limiting information may show a number of times the user is allowed to play back the digital work stored in the storage medium, the rental-shop apparatus may write the right information including the number of times the user is allowed to play back the digital work, and the playback apparatus may count a number of times the digital work has been played back every time the digital work is played back, and judge that the digital work is allowed to be used only when the counted number of times does not exceed the number of times the user is allowed to play back the digital work included in the right information.

According to this construction, the number of times playback is allowed can be set for the user who owns the semiconductor memory.

Here, the storage medium may store first identification information in correspondence with the digital content data, the first identification information identifying the digital work, the rental-shop apparatus may write the right information including second identification information into the area of the semiconductor memory, the second identification information identifying the digital work, and the playback apparatus may compare the first identification information stored in the storage medium and the second identification information included in the read right information, and only when the first identification

information and the second identification information match, judge that the digital work identified by the digital content data stored in correspondence with the first identification information is allowed to be used.

According to this construction, the playback apparatus compares the first identification information stored in the storage medium and the second identification information included in the read right information, and judges that the digital work represented by the digital content data stored in correspondence with the first identification information is allowed to be used only when the first identification information and the second identification information match. This can ensure that the use of digital work by the user who owns the semiconductor memory is limited only to digital work that is allowed to be played back.

Here, the digital content data stored in the storage medium may have been generated by encrypting the digital work using a content key, the rental-shop apparatus may securely write the right information including an encrypted content key that has been generated by encrypting the content key using a device key, into the area of the semiconductor memory, the semiconductor memory may further prestore the device key in the area, the device key being unique to the semiconductor memory, the semiconductor memory may further include a decryption unit operable to decrypt the encrypted content

key stored in the area using the device key stored in the area, to generate the content key, and output the generated content key, and the playback apparatus, upon receipt of the playback instruction from the user, may receive the content key from the semiconductor memory, and decrypt the read digital content data using the received content key, to generate the digital work.

According to this construction, the semiconductor memory prestores the device key in the area, and includes the decryption unit that decrypts the encrypted content key stored in the area using the device key to generate the content key, and outputs the generated content key. Therefore, the possibility of the decryption unit being decoded can be reduced.

Here, the digital content data stored in the storage medium may have been generated by encrypting the digital work using a content key, the storage medium may store a disc key that is unique to the storage medium, the rental shop apparatus may securely write the right information including an encrypted content key that has been generated by encrypting the content key using the disc key, into the area of the semiconductor memory, the semiconductor memory may further include a decryption unit for obtaining the disc key from the storage medium via the playback apparatus, decrypting the encrypted content key stored in the area using the obtained

disc key to generate the content key, and outputting the generated content key, and the playback apparatus, upon receipt of the playback instruction from the user, may receive the content key from the semiconductor memory, decrypt the read digital content data using the received content key, to generate the digital work.

According to this construction, the semiconductor memory obtains the disc key from the storage medium via the playback apparatus, decrypts the encrypted content key stored in the area to generate the content key, and outputs the generated content key. Therefore, even if the storage medium is copied by an unauthorized user, decryption of the encrypted content can be prevented.

Here, the semiconductor memory may perform mutual device authentication with the rental-shop apparatus, and only when the mutual device authentication succeeds, allow the rental-shop apparatus to write the right information. Also, the semiconductor memory may perform mutual device authentication with the playback apparatus, and only when the mutual device authentication succeeds, allow the playback apparatus to read the right information.

According to these constructions, the semiconductor memory and the playback apparatus perform mutual device authentication between them. Therefore, only an authenticated device is allowed to use the right information.

Here, the area of the semiconductor memory may include a plurality of application areas being provided in one-to-one correspondence with a plurality of application functions, each application area being provided for securely storing information for the corresponding application function, and

one of the plurality of application functions may be a rental function of renting the storage medium for use in the storage-medium rental system, and the application area corresponding to the rental function is used to store the right information.

According to this construction, the area of the semiconductor memory includes a plurality of application areas in one-to-one correspondence with the a plurality of application functions for securely storing information. Therefore, the semiconductor memory can be used for various purposes.

Here, another one of the plurality of application functions may be a membership card function of identifying a member of a rental shop, and the application area corresponding to the membership card function may be used to store a member number that identifies the user.

According to this construction, one of the application areas in the semiconductor memory is used to store a member number that identifies the user. Therefore, the semiconductor memory can function as a membership card for

identifying a member of the rental shop.

Here, another one of the plurality of application functions may be a bonus provision function of providing, from the rental agent to the user, point information as a bonus in accordance with use of the storage medium, and the application area corresponding to the bonus provision function may be used to store point information showing a predetermined number of points that can be used to make a payment for playback of the digital work, when the rental agent receives the payment from the user, the rental-shop apparatus may send to the semiconductor memory, a request to deduct a number of points designated by the user, from the predetermined number of points shown by the point information, as a part or all of the payment, and the semiconductor memory may further include a payment unit that deducts the designated number of points from the predetermined number of points shown by the point information, as requested by the rental-shop apparatus.

According to this construction, the semiconductor memory can function as a bonus provision card for providing, from the rental agent to the user, point information as a bonus in accordance with use of the storage medium.

Here, the rental-shop apparatus may generate, when the rental agent receives the payment from the user, point information showing a number of points in accordance with

the payment to be received, and additionally write the generated point information into the application area of the semiconductor memory.

According to this construction, the rental-shop apparatus generates, when the rental agent receives the payment from the user, point information showing the number of points in accordance with the payment to be received, and writes the generated point information to the semiconductor memory. Therefore, the user can use point information stored in the semiconductor memory.

Here, another one of the plurality of application functions may be a payment function that is used to make the payment for rental from the user to the rental agent, and the application area corresponding to the payment function may prestore electric money information showing a predetermined amount of electric money that can be used instead of actual money, when the rental agent receives the payment from the user, the rental-shop apparatus may send to the semiconductor memory, a request to deduct an amount of electric money corresponding to the payment from the predetermined amount of electric money shown by the electric money information, receive electric money information showing the amount of electric money corresponding to the payment from the semiconductor memory, and store the received electric money information, and the semiconductor memory may further

include a payment unit that transmits the electric money information showing the amount of electric money corresponding to the payment to the rental-shop apparatus as requested by the rental-shop apparatus, and deducts the amount of electric money corresponding to the payment from the predetermined amount of electric money shown by the electric money information stored in the application area.

According to this construction, when the rental agent receives the payment from the user, the rental-shop apparatus sends to the semiconductor memory, a request to deduct an amount of electric money corresponding to the payment, from the amount of electric money shown by the electric money information, and receives electric money information showing the amount of electric money corresponding to the payment from the semiconductor memory. Therefore, the user and the rental agent do not need to handle actual money.

Here, another one of the plurality of application functions may be a payment function that is used to make a payment for rental from the user to the rental agent, and the application area corresponding to the payment function may prestore electric ticket information that shows electric tickets that can be used to make a payment for playback of the digital work, when playing back the digital work, the playback apparatus may send to the semiconductor memory, a request to deduct electric tickets corresponding to the

payment determined in accordance with the playback of the digital work, from the electric tickets shown by the electric ticket information, and the semiconductor memory may further include a payment unit that deducts the electric tickets corresponding to the payment from the electric tickets shown by the electric ticket information stored in the application area, as requested by the playback apparatus.

According to this construction, when playing back the digital work, the playback apparatus sends to the semiconductor memory, a request to deduct electric tickets corresponding to the payment determined in accordance with playback of the digital work, from the electric tickets shown by the electric ticket information. Therefore, the user does not need to handle actual money at the time of playback, and the payment can be made in accordance with the playback.

Here, the playback apparatus may obtain, before playing back the digital work, electric ticket information showing remaining electric tickets from the semiconductor memory, and judge that the digital work is not allowed to be used and prohibit the digital work from being played back, when the remaining electric tickets are less than the electric tickets corresponding to the payment determined in accordance with the playback of the digital work.

According to this construction, before playing back the digital work, the playback apparatus can judge whether the

digital work is allowed to be played back or not, based on the remaining electric tickets shown by the electric ticket information stored in the semiconductor memory. Therefore, such a case can be avoided where the digital work is allowed to be played back though the remaining electric tickets are less than the required electric tickets.

Here, the playback apparatus may send to the semiconductor memory, a request to deduct electric tickets corresponding to a payment for playback of one-time from the electric tickets shown by the electric ticket information, every time the digital work is played back.

According to this construction, the playback apparatus sends to the semiconductor memory, a request to deduct electric tickets corresponding to a payment for playback of one-time from the electric tickets shown by the electric ticket information every time the digital work is played back. Therefore, the user can make a payment in accordance with the number of times the digital work is played back.

Here, when playing back the digital work one or more times during a predetermined period of time, the playback apparatus may send to the semiconductor memory, a request to deduct electric tickets corresponding to a payment for the playback of the digital work during the predetermined period of time, from the electric tickets shown by the electric ticket information.

According to this construction, when playing back the digital work one or more times during a predetermined period of time, the playback apparatus sends to the semiconductor memory, a request to deduct electric tickets corresponding to a payment for the playback of the digital work during the predetermined period of time, from the electric tickets shown by the electric ticket information. Therefore, the user can make a payment in accordance with the number of times the digital work is played back.

Brief Description of the Drawings

These and other objects, advantages and features of the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings that illustrate a specific embodiment of the invention. In the drawings:

FIG. 1 shows the construction of a rental system 1;

FIG. 2 is a block diagram showing the construction of a shop apparatus 10;

FIG. 3 shows one example of a data structure of a rental-shop membership table 151;

FIG. 4 shows one example of a data structure of a rental-use management table 152;

FIG. 5 is a block diagram showing the construction of an IC card 20;

FIG. 6 is a block diagram showing the construction of a DVD player 40;

FIG. 7 is a flowchart showing an operation performed when a member number is newly issued;

FIG. 8 is a flowchart showing an operation performed when a DVD is rented to a user who is a member of a rental shop;

FIG. 9 is a flowchart showing an operation performed when digital work stored in a DVD 30 is played back by the DVD player, continuing to FIG. 10;

FIG. 10 is a flowchart showing the operation performed when the digital work stored in the DVD 30 is played back by the DVD player, continuing from FIG. 9;

FIG. 11 is a block diagram showing the construction of a server apparatus 50;

FIG. 12 shows one example of data stored in an information storage unit 201 included in the IC card 20, and one example of data stored in the DVD 30;

FIG. 13 is a flowchart showing an operation performed when a DVD is rented to a user who is a member of a rental shop, continuing to FIG. 14;

FIG. 14 is a flowchart showing the operation performed when the DVD is rented to the user who is the member of the rental shop, continuing from FIG. 13;

FIG. 15 is a flowchart showing an operation performed

when digital work stored in the DVD 30 is played back by a DVD player, continuing to FIG. 16; and

FIG. 16 is a flowchart showing the operation performed when the digital work stored in the DVD 30 is played back by the DVD player, continuing from FIG. 15.

Best Mode for Carrying Out the Invention

1. First Embodiment

The following describes a rental system 1 as a first embodiment of the present invention.

1.1 Construction of the Rental System 1

As shown in FIG. 1, the rental system 1 is roughly composed of a shop apparatus 10, an IC card 20, a DVD 30, and a DVD player 40.

The shop apparatus 10 is located at a shop run by a rental agent, and its operations are managed by the rental agent. When the rental agent rents a user the DVD (Digital Versatile Disc) 30 storing digital work such as a movie and music, the IC card 20 owned by the user is mounted on the shop apparatus 10. The shop apparatus 10 writes rental-use management information that is described later, to the IC card 20 owned by the user.

The DVD player 40 is located at the user's home. To play back the digital work stored in the rented DVD 30, the user mounts the DVD 30 and the IC card 20 on the DVD player

40. The DVD player 40 judges whether the digital work stored in the DVD 30 is allowed to be played back or not, based on the rental-use management information stored in the IC card 20. When judging that the digital work is allowed to be played back, the DVD player 40 plays back the digital work.

The following describes each component of the rental system 1.

1.1.1 Construction of the DVD 30

The DVD 30 is an optical magnetic disc that can store high-volume information. As shown in FIG. 1, the DVD 30 is wrapped in a DVD package 31. A barcode is printed on the surface of the DVD package 31. The barcode indicates a title ID that is described later.

As one example shown in FIG. 6, the DVD 30 prestores encrypted content, an encrypted title key, and rental disc identification information.

The encrypted content is generated by encrypting content that is digital work, i.e., a movie, using a title key. The title key used to encrypt the content is unique to the content. Here, DES (Data Encryption Standard) is used as an encryption algorithm.

The encrypted title key is generated by encrypting the title key using a device key that is described later. Here, too, DES is used as an encryption algorithm.

The rental disc identification information shows that

the DVD 30 is a disc available for rental. Also, the rental disc identification information includes a title ID. Here, the title ID is identification information for identifying the original content of the encrypted content stored in the DVD 30.

1.1.2 Construction of the Shop Apparatus 10

As shown in FIG. 2, the shop apparatus 10 is roughly composed of an information storage unit 101, an input unit 102, a display unit 103, a control unit 104, an IC card reading unit 105, a barcode processing unit 106, and an authentication unit 107. Also, a barcode reader 11 is connected to the shop apparatus 10.

Specifically, the shop apparatus 10 is a computer system that is roughly composed of a microprocessor, a ROM, a RAM, a hard disk unit, a display unit, and a keyboard. The hard disk unit stores computer programs. The functions of the shop apparatus 10 are realized by the microprocessor operating in accordance with the computer programs.

(1) Information Storage Unit 101

As shown in FIG. 2, the information storage unit 101 includes a rental-shop membership table 151 and a rental-use management table 152.

(Rental-Shop Membership Table 151)

The rental-shop membership table 151 is for storing information about users who are registered as members of the

rental shop run by the rental agent. As one example shown in FIG. 3, the rental-shop membership table 151 has an area for storing a plurality of sets of membership information.

Each set of membership information corresponds to one member.

A set of membership information is made up of a member number, a member name, an address, a birth date, and a telephone number. Here, the member number is an identification number for identifying the corresponding member. The member name is a full name of the member. The address is a location of residence of the member. The birth date is a date, month, and year when the member was born. The telephone number is a number of a telephone owned by the member.

(Rental-Use Management Table 152)

The rental-use management table 152 is for storing information about DVDs that are rented from the rental shop to the user. As one example shown in FIG. 4, the rental-use management table 152 includes a plurality of sets of use management information.

Each set of use management information corresponds to one rented DVD.

A set of use management information is made up of a title ID, a member number, a rental start date, a rental end date, and a rental price. Here, the title ID is identification information for identifying content stored in the

corresponding DVD. The member number identifies a member to which the DVD is rented. The rental start date is a date when rental of the DVD is started. The rental end date is a date when the rental of the DVD is ended. The rental price shows an amount of payment for the DVD rental.

(2) Authentication Unit 107

The authentication unit 107 performs mutual device authentication with the IC card 20 via the IC card reading unit 105 when the IC card 20 is mounted on the shop apparatus 10. Here, the device authentication is of a challenge-response type. The device authentication is not described in detail here as it is well known.

The authentication unit 107 sends a success message indicating a success of the mutual device authentication to the control unit 104 when the mutual device authentication between the authentication unit 107 and the IC card 20 succeeds, and sends a failure message indicating a failure of the mutual device authentication to the control unit 104 when the mutual device authentication fails.

When the mutual device authentication fails, the shop apparatus 10 thereafter does not transmit and receive information to and from the IC card 20.

(3) IC Card Reading Unit 105

The IC card reading unit 105 bidirectionally transmits and receives information between the control unit 104 and

the IC card 20 under control by the control unit 104, and between the authentication unit 107 and the IC card 20 under control by the authentication unit 107.

(4) Barcode Reader 11

The barcode reader 11 optically reads a barcode printed on the surface of the DVD package 31, generates read-information corresponding to the barcode, and outputs the generated read-information to the barcode processing unit 106.

(5) Barcode Processing Unit 106

The barcode processing unit 106 receives the read-information from the barcode reader 11, generates a title ID using the received read-information, and outputs the generated title ID to the control unit 104.

(6) Control Unit 104

(Member Number Issuing Process)

The following describes a process of issuing a member number. In the member number issuing process, when authentication performed by the authentication unit 107 in the shop apparatus 10 succeeds and authentication performed by an authentication unit 204 in the IC card 20 succeeds, the control unit 104 receives a member name, an address, a birth date, and a telephone number from the input unit 102. Also, the control unit 104 newly generates a member number. Following this, the control unit 104 additionally writes a

set of membership information that is made up of the generated member number, the received member name, address, birth date, and telephone number, to the rental-shop membership table 151 held by the information storage unit 101.

Also, the control unit 104 outputs the generated member number to the IC card 20 via the IC card reading unit 105.

(DVD Rental Process)

The following describes a process of renting a DVD. In the DVD rental process, the control unit 104 receives a title ID from the barcode processing unit 106.

When authentication performed by the authentication unit 107 in the shop apparatus 10 succeeds and authentication performed by the authentication unit 204 in the IC card 20 succeeds, the control unit 104 outputs a request to read a member number to the IC card 20 via the IC card reading unit 105. The control unit 104 receives the member number from the IC card 20 via the IC card reading unit 105.

Following this, the control unit 104 sets a rental start date, a rental end date, and a rental price. Here, the rental start date is a date of today, and the rental end date is a date seven days after the rental start date. Also, the rental price is a predetermined value. It should be noted here that the rental end date may be set variably as requested by the user. It should also be noted here that the rental price may be set in accordance with a rental period, or may be set in

accordance with a type of digital work to be rented.

Following this, the control unit 104 generates a set of use management information that is made up of the generated title ID read by the barcode reader 11, the received member number, and the set rental start date, rental end date, and rental price, and additionally writes the generated set of use management information to the rental-use management table 152 held by the information storage unit 101.

Also, the control unit 104 outputs the title ID and the rental end date to the IC card 20 via the IC card reading unit 105.

(7) Input Unit 102 and Display Unit 103

The input unit 102 receives an input from an operator of the shop apparatus 10, and outputs the received input to the control unit 104. Also, the display unit 103 receives information to be displayed from the control unit 104, and displays the received information.

1.1.3 Construction of the IC Card 20

The IC card 20 is provided to the user as being bundled with the DVD player 40.

As shown in FIG. 5, the IC card 20 is roughly composed of an information storage unit 201, a decryption unit 202, a control unit 203, the authentication unit 204 and an IF unit 205.

It should be noted here that each block is connected

to another block by a connection line in FIG. 5. Here, each connection line indicates a path on which signals and information are transmitted. Also, a connection line with a drawing of a key, out of a plurality of connection lines connecting a block of the decryption unit 202 to other blocks, indicates a path on which information as a key is transmitted to the decryption unit 202. The same applies to other drawings.

Specifically, the IC card 20 is a computer system that is roughly composed of a microprocessor, a ROM, and a RAM. The RAM stores computer programs. The functions of the IC card 20 are realized by the microprocessor operating in accordance with the computer programs.

The following describes each component of the IC card 20.

(1) Information Storage Unit 201

The information storage unit 201 prestores a device key. The device key is unique to the IC card 20 and has been written by a manufacturer at the time of manufacturing the IC card 20.

A DVD disc including a title key encrypted using this device key is available for rental to the user at the rental shop.

It should be noted here that a producer of a DVD disc, more specifically a copyright-protected licenser, manages

values of all the device keys. The copyright-protected licenser distributes these device keys to the manufacturer of IC cards to be mounted on DVD players. A device key distributed from the copyright-protected licenser to the manufacturer in this way is written to an IC card by the manufacturer of the IC card.

As described above, such an IC card that includes a device key necessary for encrypting content is originally utilized in a copyright protection system, and is diverted to the rental system.

Also, the information storage unit 201 has an area for storing a member number and rental-use management information. Here, the member number is an identification number for identifying a user registered as a member. The rental-use management information is information about use of a rented DVD, more specifically, information about a title ID and a rental end date of the rented DVD.

(2) IF Unit 205

The IF unit 205 bidirectionally transmits and receives information between the control unit 203 and an external device on which the IC card 20 is mounted under control by the control unit 203, and between the authentication unit 204 and an external device on which the IC card 20 is mounted under control by the authentication unit 204. Here, an external device is the shop apparatus 10 or the DVD player 40.

(3) Authentication Unit 204

The authentication unit 204 performs mutual device authentication with the shop apparatus 10 via the IF unit 205 when the IC card 20 is mounted on the shop apparatus 10. Here, the device authentication is of a challenge-response type. The device authentication is not described in detail here as it is well known.

The authentication unit 204 sends a success message indicating a success of the mutual device authentication to the control unit 203 when the mutual device authentication between the authentication unit 204 and the shop apparatus 10 succeeds, and sends a failure message indicating a failure of the mutual device authentication to the control unit 203 when the mutual device authentication fails.

When the mutual device authentication fails, the IC card 20 thereafter does not transmit and receive information to and from the shop apparatus 10.

Also, the authentication unit 204 performs mutual device authentication with the DVD player 40 via the IF unit 205 when the IC card 20 is mounted on the DVD player 40. Here, the device authentication is of a challenge-response type. The device authentication is not described in detail here as it is well known.

The authentication unit 204 sends a success message indicating a success of the mutual device authentication to

the control unit 203 when the mutual device authentication between the authentication unit 204 and the DVD player 40 succeeds, and sends a failure message indicating a failure of the mutual device authentication to the control unit 203 when the mutual device authentication fails.

When the mutual device authentication fails, the IC card 20 thereafter does not transmit and receive information to and from the DVD player 40.

(4) Decryption Unit 202

The decryption unit 202 receives an encrypted title key from the control unit 203, reads a device key from the information storage unit 201, decrypts the received encrypted title key using the read device key to generate a title key, and outputs the generated title key to the control unit 203. Here, DES is used as a decryption algorithm.

(5) Control Unit 203

(Member Number Issuing Process)

To newly issue a member number, the control unit 203 receives a member number from the shop apparatus 10 via the IF unit 205, and writes the received member number to the information storage unit 201.

(DVD Rental Process)

To rent a DVD to a user who is a member of the rental shop, the control unit 203 receives a request to read a member number via the IF unit 205 when authentication performed by

the authentication unit 107 in the shop apparatus 10 succeeds and authentication performed by the authentication unit 204 in the IC card 20 succeeds. Upon receipt of the request, the control unit 203 reads the member number from the information storage unit 201, and outputs the read member number to the shop apparatus 10 via the IF unit 205.

Also, the control unit 203 receives a title ID and a rental end date from the shop apparatus 10 via the IF unit 205. Following this, the control unit 203 writes rental-use management information including the received title ID and the rental end date to the information storage unit 201.

(DVD Playback Process)

The following describes a DVD playback process in which the user to which the DVD 30 has been rented plays back digital work stored in the DVD 30. In the DVD playback process, the control unit 203 first receives rental disc identification information from the DVD player 40 via the IF unit 205 when authentication performed by the authentication unit 406 in the DVD player 40 succeeds and authentication performed by the authentication unit 204 in the IC card 20 succeeds.

Following this, the control unit 203 reads a title ID included in rental-use management information from the information storage unit 201, and judges whether the title ID included in the received rental disc identification information and the read title ID match or not. When a result

of this judgment is negative, the control unit 203 ends the process.

When the result of the above judgment is affirmative, the control unit 203 sends a request to obtain the present date and time, to the DVD player 40 via the IF unit 205. Then, the control unit 203 receives the present date and time from the DVD player 40 via the IF unit 205.

Following this, the control unit 203 reads a rental end date included in the rental-use management information from the information storage unit 201, and compares the received present date and time and the read rental end date. When judging that the present date and time is after the rental end date, the control unit 203 ends the process.

When judging that the present date and time is before the rental end date or is on the rental end date, the control unit 203 sends a request to read an encrypted title key from the DVD 30, via the IF unit 205, to the DVD player 40. Then, the control unit 203 receives the encrypted title key from the DVD player 40 via the IF unit 205, and outputs the received encrypted title key to the decryption unit 202. The control unit 203 receives a title key from the decryption unit 202, and outputs the received title key to the DVD player 40 via the IF unit 205.

1.1.4 Construction of the DVD Player 40

As shown in FIG. 6, the DVD player 40 is roughly composed

of an input unit 401, a decoder 402, a decryption unit 403, a control unit 404, a clock unit 405, the authentication unit 406, and an IF unit 407.

Specifically, the DVD player 40 is a computer system that is roughly composed of a microprocessor, a ROM, and a RAM. The ROM stores computer programs. The functions of the DVD player 40 are partially realized by the microprocessor operating in accordance with the computer programs.

(1) Input Unit 401

The input unit 401 reads information from the DVD 30 under control by the control unit 404 or the decryption unit 403, and outputs the read information to the control unit 404 or the decryption unit 403.

(2) IF Unit 407

The IF unit 407 bidirectionally transmits and receives information between the control unit 404 and the IC card 20 under control by the control unit 404, and between the authentication unit 406 and the IC card 20 under control by the authentication unit 406.

(3) Authentication Unit 406

The authentication unit 406 performs mutual device authentication with the IC card 20 via the IF unit 407 when the IC card 20 is mounted on the DVD player 40. Here, the device authentication is of a challenge-response type. The device authentication is not described in detail here as it

is well known.

The authentication unit 406 sends a success message indicating a success of the mutual device authentication to the control unit 404 when the mutual device authentication between the authentication unit 406 and the IC card 20 succeeds, and sends a failure message indicating a failure of the mutual device authentication to the control unit 404 when the mutual device authentication fails.

When the mutual device authentication fails, the DVD player 40 thereafter does not transmit and receive information to and from the IC card 20.

(4) Clock Unit 405

The clock unit 405 clocks the present date and time, and outputs the present date and time to the control unit 404 as requested by the control unit 404.

(5) Decryption Unit 403

The decryption unit 403 receives a title key from the control unit 404, reads encrypted content from the DVD 30 via the input unit 401, decrypts the read encrypted content using the received title key to generate content, and outputs the generated content to the decoder 402. Here, DES is used as a decryption algorithm.

(6) Decoder 402

The decoder 402 receives content from the decryption unit 403, plays back the received content to generate video

and audio signals, and outputs the generated video and audio signals to the monitor 41. The monitor 41 receives the video and audio signals, converts the video and audio signals into video and audio, and outputs the video and audio.

(7) Control Unit 404

The control unit 404 reads rental disc identification information from the DVD 30 via the input unit 401 and outputs the read rental disc identification information to the IC card 20 via the IF unit 407 when authentication performed by the authentication unit 406 in the DVD player 40 succeeds and authentication performed by the authentication unit 204 in the IC card 20 succeeds.

Also, the control unit 404 receives a request to obtain the present date and time from the IC card 20 via the IF unit 407. Upon receipt of the request, the control unit 404 obtains the present date and time from the clock unit 405, and outputs the obtained present date and time to the IC card 20 via the IF unit 407.

Also, the control unit 404 receives a request to read an encrypted title key from the DVD 30, from the IC card 20 via the IF unit 407. Upon receipt of the request, the control unit 404 reads the encrypted title key from the DVD 30, and outputs the read encrypted title key to the IC card 20 via the IF unit 407.

Further, the control unit 404 receives the title key

from the IC card 20 via the IF unit 407, and outputs the received title key to the decryption unit 403.

1.2 Operation of the Rental System 1

The following describes an operation of each of the member number issuing process, the DVD rental process, and the DVD playback process in the rental system 1.

1.2.1 Member Number Issuing Process

The following describes an operation performed when a member number is newly issued, with reference to a flowchart shown in FIG. 7.

A shop clerk who operates the shop apparatus 10 at the rental shop receives the IC card 20 from a user who wants to newly register as a member of the rental shop, and mounts the received IC card 20 on the shop apparatus 10.

When the IC card 20 is mounted on the shop apparatus 10 by the operator of the shop apparatus 10, the authentication unit 107 in the shop apparatus 10 performs authentication of the authentication unit 204 in the IC card 20 (step S101), and the authentication unit 204 in the IC card 20 performs authentication of the authentication unit 107 in the shop apparatus 10 (step S111).

When the authentication performed by the authentication unit 107 in the shop apparatus 10 fails (step S102), the shop apparatus 10 thereafter stops processing relating to the IC card 20 and ends the member number issuing process. Also,

when the authentication performed by the authentication unit 204 in the IC card 20 fails (step S112), the IC card 20 stops processing relating to the shop apparatus 10.

When the authentication performed by the authentication unit 107 in the shop apparatus 10 succeeds (step S102), and the authentication performed by the authentication unit 204 in the IC card 20 succeeds (step S112), the input unit 102 receives an input of a member name, outputs the input member name to the control unit 104 (step S103), receives an input of an address and a telephone number, outputs the input address and telephone number to the control unit 104 (step S104), receives an input of a birth date, and outputs the input birth date to the control unit 104 (step S105). Following this, the control unit 104 generates a new member number (step S106), and writes a set of membership information that is made up of the generated member number, and the received member name, address, birth date, and telephone number, to the rental-shop membership table 151 held by the information storage unit 101 (step S107).

Following this, the control unit 104 outputs the generated member number to the IC card 20 via the IC card reading unit 105, and the control unit 203 in the IC card 20 receives the member number via the IF unit 205 (step S108). The control unit 203 writes the received member number to the information storage unit 201 (step S113).

As described above, a set of membership information for the user who has newly become a member is registered in the shop apparatus 10, and the user's member number is stored into the IC card 20 that is owned by the user.

1.2.2 DVD Rental Process

The following describes an operation performed when a DVD is rented to a user who is a member of the rental shop, with reference to a flowchart shown in FIG. 8.

A shop clerk who operates the shop apparatus 10 at the rental shop operates the barcode reader 11 so as to optically read a barcode printed on the surface of the DVD package 31.

The barcode reader 11 connected to the shop apparatus 10 optically reads the barcode printed on the surface of the DVD package 31, and generates read-information corresponding to the read barcode (step S121). The barcode processing unit 106 receives the read-information from the barcode reader 11, generates a title ID using the received read-information, and outputs the generated title ID to the control unit 104 (step S122).

Following this, the shop clerk who operates the shop apparatus 10 receives the IC card 20 from the user who is a member of the rental shop, and mounts the received IC card 20 on the shop apparatus 10.

When the IC card 20 is mounted on the shop apparatus 10 by the operator of the shop apparatus 10, the authentication

unit 107 in the shop apparatus 10 performs authentication of the authentication unit 204 in the IC card 20 (step S123), and the authentication unit 204 in the IC card 20 performs authentication of the authentication unit 107 in the shop apparatus 10 (step S131).

When the authentication performed by the authentication unit 107 in the shop apparatus 10 fails (step S124), the shop apparatus 10 thereafter stops processing relating to the IC card 20 and ends the DVD rental process. Also, when the authentication performed by the authentication unit 204 in the IC card 20 fails (step S132), the IC card 20 stops processing relating to the shop apparatus 10.

When the authentication performed by the authentication unit 107 in the shop apparatus 10 succeeds (step S124), and the authentication performed by the authentication unit 204 in the IC card 20 succeeds (step S132), the control unit 104 outputs a request to read a member number, to the IC card 20 via the IC card reading unit 105, and the control unit 203 receives the request to read the member number via the IF unit 205 (step S125). Upon receipt of the request to read the member number, the control unit 203 reads the member number from the information storage unit 201 (step S133), and outputs the read member number to the shop apparatus 10 via the IF unit 205. The control unit 104 receives the member number via the IC card reading unit 105 (step S134).

Following this, the control unit 104 sets a rental start date, a rental end date, and a rental price, generates a set of use management information that is made up of the generated title ID read by the barcode reader 11, the received member number, and the set rental start date, rental end date, and rental price, and additionally writes the generated set of use management information to the rental-use management table 152 held by the information storage unit 101 (step S126). Following this, the control unit 104 outputs the title ID and the rental end date to the IC card 20 via the IC card reading unit 105. The control unit 203 receives the title ID and the rental end date via the IF unit 205 (step S127).

Then, the control unit 203 writes rental-use management information including the received title ID and rental end date, to the information storage unit 201 (step S135).

As described above, rental-use management information relating to the DVD 30 to be rented to the user is written to the IC card 20 that is owned by the user.

1.2.3 DVD Playback Process

The following describes an operation performed when the user to which the DVD 30 has been rented plays back digital work stored in the DVD 30, with reference to a flowchart shown in FIGS. 9 and 10.

The user to which the DVD 30 has been rented mounts the DVD 30 and the IC card 20 on the DVD player 40.

When the IC card 20 is mounted on the DVD player 40 by the user, the authentication unit 406 in the DVD player 40 performs authentication of the authentication unit 204 in the IC card 20 (step S141), and the authentication unit 204 in the IC card 20 performs authentication of the authentication unit 406 in the DVD player 40 (step S151).

When the authentication performed by the authentication unit 406 in the DVD player 40 fails (step S142), the DVD player 40 thereafter stops processing relating to the IC card 20 and ends the DVD playback process. Also, when the authentication performed by the authentication unit 204 in the IC card 20 fails (step S152), the IC card 20 stops processing relating to the DVD player 40.

When the authentication performed by the authentication unit 406 in the DVD player 40 succeeds (step S142), and the authentication performed by the authentication unit 204 in the IC card 20 succeeds (step S152), the control unit 404 reads rental disc identification information from the DVD 30 via the input unit 401 (step S143). The control unit 404 outputs the read rental disc identification information to the IC card 20 via the IF unit 407, and the control unit 203 receives the rental disc identification information via the IF unit 205 (step S144).

Following this, the control unit 203 reads a title ID included in rental-use management information from the

information storage unit 201, and judges whether the title ID included in the received rental disc identification information and the read title ID match or not. When a result of this judgment is negative (step S153), the control unit 203 ends the process.

When the result of the above judgment is affirmative (step S153), the control unit 203 sends a request to obtain the present date and time to the DVD player 40 via the IF unit 205. The control unit 404 receives the request to obtain the present date and time via the IF unit 407 (step S154). The control unit 404 then obtains the present date and time from the clock unit 405 (step S145), and outputs the obtained present date and time to the IC card 20 via the IF unit 407. The control unit 203 receives the present date and time via the IF unit 205 (step S146).

Following this, the control unit 203 reads a rental end date included in the rental-use management information from the information storage unit 201, and compares the received present date and time with the read rental end date. When judging that the present date and time is after the rental end date (step S155), the control unit 203 ends the process.

When judging that the present date and time is before the rental end date or is on the rental end date (step S155), the control unit 203 sends a request to read an encrypted title key from the DVD 30, to the DVD player 40 via the IF

unit 205. The control unit 404 receives the request via the IF unit 407 (step S171). Then, the control unit 404 reads the encrypted title key from the DVD 30, and outputs the read encrypted title key to the IC card 20 via the IF unit 407. The control unit 203 receives the encrypted title key via the IF unit 205, and outputs the encrypted title key to the decryption unit 202 (step S162).

Following this, the decryption unit 202 reads a device key from the information storage unit 201 (step S172), and decrypts the received encrypted title key using the read device key, to generate a title key (step S173). The control unit 203 outputs the generated title key to the DVD player 40 via the IF unit 205, and the control unit 404 receives the title key via the IF unit 407 (step S174).

Following this, the control unit 404 outputs the received title key to the decryption unit 403. The decryption unit 403 reads encrypted content from the DVD 30 via the input unit 401 (step S163), decrypts the read encrypted content using the received title key to generate content, and outputs the generated content to the decoder 402 (step S164). The decoder 402 receives the content, and plays back the received content to output video and audio signals to the monitor 41. The monitor 41 receives the video and audio signals and outputs them in the form of video and audio (step S165).

In the above-described way, the user can play back digital

work stored in the DVD 30.

1.3 Conclusions

As described above, in the storage-medium rental system relating to the present embodiment, the rental agent rents the user a storage medium storing digital work, so as to provide the digital work to the user.

To be more specific, the rental system is for temporarily providing a right to use the digital work stored in the storage medium from the rental agent to the user.

The rental system is roughly composed of a portable storage medium to be rented (specifically, a DVD), a portable semiconductor memory (an IC card), a shop apparatus, and a playback apparatus (a DVD player).

The portable storage medium prestores digital content data representing digital work. The portable semiconductor memory has an area for securely storing information. The shop apparatus securely writes into the area of the semiconductor memory, right information that shows a range of the right to use the digital work stored in the storage medium, when the rental agent rents the user the storage medium. Upon receipt of an instruction to play back the digital work from the user, the playback apparatus securely reads the right information from the area of the semiconductor memory, and judges whether the digital work is allowed to be used or not, based on the read right information. Only when judging that

the digital work is allowed to be used, the playback apparatus reads the digital content data from the storage medium, and plays back the digital work, based on the read digital content data.

As can be known from the above, the IC card is an essential component for the playback apparatus to play back the content stored in the DVD. This can produce the following effect. Suppose that an unauthorized user with a malicious intention shoplifts a DVD disc displayed at the rental shop and brings the DVD home. In this case, the user cannot play back content stored in the DVD disc because the user's IC card does not store authenticated information.

Further, the DVD player may be equipped with only one reading unit for an IC card. This reading unit is originally provided to read and write information to and from an IC card for use in the copyright protection system. This reading unit can also read and write information to and from an IC card diverted to the rental system. Accordingly, the DVD player does not need to be newly equipped with another reading unit specially for an IC card used in the rental system.

Moreover, the rental shop can use a membership card also as a rental card, and so, the operating cost relating to these cards can be reduced.

Also, the user does not have to carry a plurality of cards for these purposes.

2. Second Embodiment

The following describes a rental system 1a (not shown) as a modification of the rental system 1 described in the first embodiment.

2.1 Construction of the Rental System 1a

The rental system 1a is roughly composed of a shop apparatus 10, an IC card 20, a DVD 30, a DVD player 40, and a server apparatus 50.

The shop apparatus 10, the IC card 20, the DVD 30, and the DVD player 40 in the rental system 1a respectively have the same constructions as the shop apparatus 10, the IC card 20, the DVD 30, and the DVD player 40 in the rental system 1.

The following describes the rental system 1a in the present embodiment, focusing on its differences from the rental system 1.

2.1.1 DVD 30

As shown in FIG. 12, the DVD 30 prestores encrypted content and rental disc identification information.

The DVD 30 in the second embodiment differs from the DVD 30 in the first embodiment in that it does not store an encrypted title key.

2.1.2 Server Apparatus 50

As shown in FIG. 11, the server apparatus 50 is roughly

composed of an information storage unit 501, a transmission/reception unit 502, a control unit 503, and a display unit and an input unit that are not shown. The server apparatus 50 is connected to the shop apparatus 10 via a communication line 60.

Specifically, the server apparatus 50 is a computer system that is roughly composed of a microprocessor, a ROM, a RAM, a hard disk unit, a display unit, a keyboard, a mouse, and a communication-line connecting unit. The hard disk unit stores computer programs. The functions of the server apparatus 50 are realized by the microprocessor operating in accordance with the computer programs.

(1) Information Storage Unit 501

As one example shown in FIG. 11, the information storage unit 501 stores a title table 521.

The title table 521 includes a plurality of sets of title information, each of which is made up of a title ID, a device key identifier, and an encrypted title key.

The title ID is identification information for identifying content that is digital work stored in the DVD 30.

The device key identifier is identification information for identifying a device key stored in the information storage unit 201 in the IC card 20.

The encrypted title key is generated by encrypting a

title key using a device key identified by the device key identifier. Here, the title key is used to encrypt content i.e., digital work, identified by the title ID.

(2) Control Unit 503

The control unit 503 receives a request to obtain an encrypted title key from the shop apparatus 10 via the communication line 60 and the reception/transmission unit 502. The control unit 503 further receives a title ID and a device key identifier.

Upon receipt of the request, the control unit 503 reads an encrypted title key corresponding to the received title ID and device key identifier, from the title table 521 held by the information storage unit 501. Following this, the control unit 503 outputs the read encrypted title key to the shop apparatus 10 via the transmission/reception unit 502 and the communication line 60.

(3) Transmission/Reception Unit 502

The transmission/reception unit 502 is connected to the shop apparatus 10 via the communication line 60. The transmission/reception unit 502 transmits and receives information between the control unit 503 and the shop apparatus 10 via the communication line 60.

2.1.3 IC Card 20

(1) Information Storage Unit 201

As shown in FIG. 12, the information storage unit 201

further prestores a device key identifier for identifying a device key. The device key identifier has been written thereto by the manufacture at the time of manufacturing the IC card 20.

(2) Control Unit 203

In the DVD rental process, the control unit 203 receives a request to obtain a device key identifier from the shop apparatus 10 via the IF unit 205. Upon receipt of the request, the control unit 203 reads the device key identifier from the information storage unit 201, and outputs the read device key identifier to the shop apparatus 10 via the IF unit 205.

Also, in the DVD rental process, the control unit 203 receives an encrypted title key as one item of rental-use management information, from the shop apparatus 10 via the IF unit 205, and writes the received encrypted title key to the information storage unit 201 as one item of the rental-use management information.

Further, in the DVD playback process, the control unit 203 reads an encrypted title key from the rental-use management information stored in the information storage unit 201. The control unit 203 decrypts the read encrypted title key using the device key read from the information storage unit 201, to generate a title key.

The control unit 203 in the first embodiment obtains the encrypted title key from the DVD 30 via the DVD player

40. Unlike in the first embodiment, however, the control unit 203 in the second embodiment reads the encrypted title key from the information storage unit 201.

2.1.4 Shop Apparatus 10

(1) Control Unit 104

In the DVD rental process, the control unit 104 outputs a request to obtain a device key identifier to the IC card 20 via the IC card reading unit 105.

The control unit 104 receives a device key identifier from the IC card 20 via the IC card reading unit 105.

Following this, the control unit 104 outputs a request to obtain an encrypted title key to the server apparatus 50 via the communication line 60. The control unit 104 further outputs a title ID read by the barcode reader 11 and a device key identifier obtained from the IC card 20, to the server apparatus 50 via the communication line 60.

The control unit 104 then receives an encrypted title key from the server apparatus 50 via the communication line 60.

Following this, the control unit 104 outputs a title ID, a rental end date, and an encrypted title key, to the IC card 20 via the IC card reading unit 105.

2.2 Operation of the Rental System 1a

The following describes an operation of the rental system 1a, focusing on its differences from the operation of the

rental system 1 in the first embodiment.

2.2.1 DVD Rental Process

The following describes an operation performed when a DVD is rented to the user who is a member of the rental shop, with reference to a flowchart shown in FIGS. 13 and 14, focusing on its differences from the operation shown in FIG. 8.

The control unit 104 writes the generated set of use management information to the rental-use management table 152 in step S126. Then, the control unit 104 outputs a request to obtain a device key identifier to the IC card 20 via the IC card reading unit 105 (step S201). The control unit 203 then reads the device key identifier from the information storage unit 201 (step S202), and outputs the read device key identifier to the shop apparatus 10 via the IF unit 205 (step S203).

Following this, the control unit 104 outputs the request to obtain the encrypted title key to the server apparatus 50 via the communication line 60 (step S204). The control unit 104 further outputs the title ID read by the barcode reader 11 and the device key identifier obtained from the IC card 20 to the server apparatus 50 via the communication line 60 (step S205).

The control unit 503 reads an encrypted title key corresponding to the received title ID and device key identifier from the title table 521 held by the information

storage unit 501 (step S206). Following this, the control unit 503 outputs the read encrypted title key to the shop apparatus 10 via the transmission/reception unit 502 and the communication line 60 (step S207).

Upon receipt of the encrypted title key from the server apparatus 50 via the communication line 60 (step S207), the control unit 104 outputs the title ID, the rental end date, and the encrypted title key to the IC card 20 via the IC card reading unit 105 (step S208).

Following this, the control unit 203 writes the received encrypted title key to the information storage unit 201 as one item of the rental-use management information (step S209).

2.2.2 DVD Playback Process

The following describes an operation performed when the user to which the DVD 30 has been rented plays back digital work stored in the DVD 30, with reference to a flowchart shown in FIGS. 15 and 16, focusing on its differences from the operation shown in FIGS. 9 and 10.

When judging that the title ID included in the received rental disc identification information and the read title ID match in step S153, the control unit 203 reads an encrypted title key from rental-use management information stored in the information storage unit 201 (step S221). Following this, the control unit 203 reads a device key in step S172.

2.3 Conclusions

As described above, unlike in the first embodiment where an encrypted title key is stored in a DVD disc, in the second embodiment a DVD disc available for rental does not store an encrypted title key, and the shop apparatus 10 writes the encrypted title key to the IC card 20 at the rental shop when the DVD disc is rented.

Further, a device key identifier for identifying a device key has been additionally written to the IC card 20 at the time of manufacturing the IC card 20.

The server apparatus 50 stores an encrypted title key in correspondence with a title ID and a device key.

When a DVD disc is rented, the shop apparatus 10 reads a device key identifier from the IC card 20, obtains an encrypted title key from the server apparatus 50, and writes the obtained encrypted title key to the IC card 20 as one item of rental-use management information.

When a DVD disc is played, content stored in the DVD disc is played back based on a title ID stored in the DVD disc, in the same manner as in the first embodiment. Here, the DVD player 40 obtains an encrypted title key from the IC card 20.

3. Other Modifications

3.1 Modifications 1

Although the first embodiment describes the case where the shop apparatus 10 writes a rental end date to the IC card

20, the following modifications are also possible.

(1) Although the DVD player 40 internally has the clock unit 405 for clocking a date and time, the DVD player 40 may obtain the present date and time from an external device via a network.

(2) The above-described rental end date is a final date of a rental period during which rental is allowed, i.e., the rental end date is an absolute expiry date of the rental period. Instead of such a rental end date, the shop apparatus 10 may write a rental start date and period information showing a rental period starting from the rental start date, to the IC card 20. In this case, the DVD player 40 judges whether playback is allowed or not, using the rental start date, the period information, and the present date and time.

Also, the shop apparatus 10 may write period information showing a rental period starting from a date and time when content is firstly played back, to the IC card 20. In this case, the DVD player 40 records the date and time when the content is firstly played back and judges whether playback of the content is allowed or not, using the recorded date and time, the period information, and the present date and time.

Further, the shop apparatus 10 may write the number of times digital work stored in the storage medium is allowed to be played back, to the IC card 20. In this case, the DVD

player 40 counts the number of times the digital work has been played back. The DVD player 40 judges that the digital work is allowed to be played back, only when the counted number of times does not exceed the allowable number of times included in the right information.

3.2 Modifications 2

Although the first embodiment describes the case where an encrypted title key generated by encrypting a title key using a device key unique to the IC card 20 is used, the following modifications are also possible.

The DVD 30 prestores a medium identifier unique to the DVD 30. Because the medium identifier is unique to the DVD 30, this medium identifier is not copied even if encrypted content and the like stored in the DVD 30 are copied into another DVD-RW or the like. The other DVD-RW or the like stores its own unique medium identifier that is different from the above medium identifier unique to the DVD 30.

The server apparatus stores a title ID, a medium identifier, and an encrypted title key in correspondence with one another. The title ID is identification information for identifying content that is digital work. The medium identifier is an identifier for identifying a DVD storing content identified by the title ID. The encrypted title key is generated by encrypting a title key using the medium identifier as a key.

When the DVD 30 is rented, the shop apparatus 10 writes an encrypted title key stored in correspondence with a title ID identifying content stored in a DVD to be rented from the server apparatus, to the IC card 20, as one item of rental-use management information.

To play back encrypted content stored in the DVD 30, the DVD player 40 obtains the encrypted title key from the IC card 20, obtains a medium identifier from the DVD 30, and decrypts the encrypted title key using the obtained medium identifier, to generate a title key. Then, using the generated title key, the DVD player 40 decrypts the encrypted content stored in the DVD 30, to generate content, and outputs the generated content.

As described above, a key that is used to encrypt a title key to generate an encrypted title key is a medium identifier stored in the DVD 30. Therefore, even if information stored in the DVD 30 is copied to another DVD by an unauthorized user, a medium identifier that is read from the other DVD is not the same as the above medium identifier. Therefore, the encrypted title key cannot be decrypted properly. As a result, the encrypted content cannot be decrypted properly. In this way, unauthorized playback of content by such an unauthorized user who copies information stored in the DVD 30 to another DVD can be prevented.

3.3 Modifications 3

The IC card 20 can be used for various applications. Examples of the various applications include a DVD rental function, a membership card function, a point provision function, a credit card function, an electric money function, and a prepaid card function.

The information storage unit 201 in the IC card 20 includes a plurality of application areas for securely storing information in one-to-one correspondence with a plurality of application functions. Each application area stores information to be utilized by the corresponding application function.

(Membership Card Function)

One of the application functions is a membership card function of identifying a member of the rental shop. The application area corresponding to the membership card function is used to store a member number that identifies the user.

The membership card function is described in the first embodiment.

(Bonus Provision Function for Providing Point Information)

Another one of the application functions is a bonus provision function of providing, from the rental agent to the user, point information as a membership bonus, in accordance with use of the DVD. The information storage unit 201 in the IC card 20 includes one application area corresponding to the bonus provision function. The shop

apparatus 10 additionally writes, to the application area, point information showing the number of points determined in accordance with DVD rental, i.e., in accordance with a payment for playback of the digital work stored in the DVD, or a payment for a product purchase.

To collect the payment from the user, the shop apparatus 10 sends to the IC card 20, a request to deduct the number of points designated by the user from the number of points shown by the point information stored in the application area, as a part or all of the payment. The IC card 20 deducts the number of points designated by the user from the number of points shown by the point information, as requested by the shop apparatus 10.

(Electric Money Function)

Another one of the application function is a payment function, i.e., an electric money function, for the user to make a payment for rental to the rental agent. The information storage unit 201 in the IC card 20 includes one application area corresponding to the electric money function. The application area prestores electric money information showing a predetermined amount of electric money that can be used instead of actual money.

To collect the payment from the user, the shop apparatus 10 sends to the IC card 20, a request to obtain electric money information showing an amount of electric money corresponding

to the payment from the IC card 20.

The IC card 20 includes the following payment unit. In response to the request from the shop apparatus 10, the payment unit transmits the electric money information showing the amount of electric money corresponding to the payment, to the shop apparatus 10, and deducts the amount of electric money corresponding to the payment from the amount of money shown by the electric money information stored in the application area.

The shop apparatus 10 receives the electric money information showing the amount of electric money corresponding to the payment from the IC card 20, and stores the received electric money information.

(Prepaid Card Function)

Another one of the application functions is a payment function, i.e., a prepaid card function, for the user to make a payment for rental to the rental agent. The information storage unit 201 in the IC card 20 includes one application area corresponding to the prepaid card function. The application area prestores electric ticket information showing electric tickets that can be used to pay for playback of the digital work.

When playing back the digital work stored in the DVD 30, the DVD player 40 sends to the IC card 20, a request to deduct electric tickets corresponding to a payment determined

in accordance with playback of the digital work, from the electric tickets shown by the electric ticket information stored in the application area.

Here, the DVD player 40 obtains information about the remaining electric tickets shown by the electric ticket information stored in the IC card 20, before playing back the digital work stored in the DVD 30. When the remaining electric tickets are less than the electric tickets corresponding to the payment determined in accordance with the playback of the digital work, the DVD player 40 judges that the digital work is not allowed to be used, and so prohibits playback of the digital work. In the other cases, the DVD player 40 judges that the digital work is allowed to be used.

Also, the DVD player 40 may send to the IC card 20, a request to deduct electric tickets corresponding to a payment for playback of one-time from the electric tickets shown by the electric ticket information stored in the application area, every time the digital work is played back. Alternatively, when the digital work is played back one or more times during a predetermined period of time, the DVD player 40 may send to the IC card 20, a request to deduct electric tickets corresponding to a payment for playback of one or more times during the predetermined period of time, from the electric tickets shown by the electric ticket information stored in the application area.

The IC card 20 includes a payment unit that deducts the electric tickets corresponding to the payment from the electric tickets shown by the electric ticket information stored in the application area, as requested by the DVD player 40.

3.4 Other Modifications

The following modifications are also possible.

(1) A DVD may store a plurality of content IDs, the same number of encrypted contents, the same number of encrypted content keys, and one encrypted disc key. The plurality of content IDs, the encrypted contents, and the encrypted content keys respectively correspond to one another.

The encrypted contents are each generated by encrypting a different content using a different content key.

The encrypted content keys are each generated by encrypting a different content key using one disc key.

The encrypted disc key is generated by encrypting the disc key using one device key.

The disc key is unique to a DVD of one type.

The device key is unique to one IC card, and is stored in the IC card.

To play back encrypted content stored in a DVD, the IC card obtains an encrypted disc key and an encrypted content key corresponding to the content to be played back, from the DVD player. The IC card then internally reads a device key,

and decrypts the encrypted disc key using the read device key, to generate a disc key. The IC card then decrypts the encrypted content key using the generated disc key to generate a content key, and outputs the generated content key to the DVD player.

The DVD player receives the content key, and decrypts the encrypted content read from the DVD using the received content key, to generate content.

(2) Although the above embodiments describe the case where a DVD storing encrypted digital content is rented, a storage medium to be rented should not be limited to a DVD. For example, a CD-ROM, a DVD-ROM, a DVD-RAM, and a BD (Blu-ray Disc) may be used.

(3) Although the above embodiments describe the case where DES is used as an encryption algorithm and a decryption algorithm, other encryption techniques may be used.

(4) The shop apparatus may have a register function of calculating amounts of money involved in transaction.

(5) Although the second embodiment describes the case where the server apparatus 50 is located distant from the rental shop, the invention should not be limited to such. For example, the server apparatus 50 may be located in the rental shop where the shop apparatus 10 is located, or the shop apparatus 10 and the server apparatus 50 may be integrated into one apparatus.

(6) Although the first and second embodiments describe the case where the rental agent rents a DVD storing digital work such as music and movies to the user, the rental agent may sell such a DVD to the user.

In this case, at the time of selling a DVD, the control unit 104 of the shop apparatus 10 generates a rental end date showing "no-time-limit" in step S126 of the flowchart shown in FIG. 8. As one example, the control unit 104 may generate, as the rental end date showing "no-time-limit", a large value "9999.99.99" indicating a date that does not actually exist. Following this, the control unit 104 generates a set of use management information including the generated rental end date, and additionally writes the generated set of use management information to the rental-use management table 152 held by the information storage unit 101.

In step S127, the control unit 104 outputs the title ID, and the rental end date showing "no-time-limit" to the IC card 20 via the IC card reading unit 105, and the control unit 203 of the IC card 20 receives the title ID and the rental end date via the IF unit 205 (step S127).

Following this, at the time of playing back the DVD, the control unit 203 of the IC card 20 reads the rental end date included in the rental-use management information from the information storage unit 201, and compares the received present date and the read rental end date in step S155 of

the flowchart shown in FIG. 9. With the rental end date showing the value "9999.99.99", the control unit 203 judges, in any cases, that the present date is before the rental end date. Therefore, the processing advances to step S171. The content is then decrypted and played back according to the procedure shown in the flowchart in FIG. 10 (steps S171 to S174 and S161 to S165).

In this way, the rental system described in the first and second embodiments enables not only renting of work but also selling of work.

This modification exemplifies the case where renting without any time limit, in other words, selling, is realized by writing a rental end date showing "no-time-limit" to the IC card. Instead of writing such a rental end date showing "no-time-limit" to the IC card, however, a flag indicating "selling" may be written to the IC card in correspondence with the title ID. In this case, when the flag indicating "selling" is written in the IC card, the comparison in step S155 is not performed. Without the comparison, the processing directly advances to step S171. The content is then decrypted and played back according to the procedure shown the flowchart in FIG. 10.

(7) The following modification is also possible in the case where the rental agent sells a DVD storing digital work such as music and movies to the user in the first end second

embodiments.

Here, a DVD for rental and a DVD for sale are assumed to be different storage mediums.

A DVD for rental internally stores encrypted content, an encrypted title key, and rental disc identification information as shown in FIG. 6. As described above, the rental disc identification information indicates that the DVD is a rental disc.

On the other hand, a DVD for sale stores media unique information unique to the DVD in its area that is not rewritable by an external device. A DVD for sale further internally stores encrypted content, an encrypted title key, and sales disc identification information. The encrypted content has been generated by encrypting, using a title key, content that is digital work, i.e., a movie. The title key is an encryption key unique to the content. The encrypted title key has been generated by encrypting the title key using the media unique information. The sales disc identification information indicates that the DVD is a sales disc.

The DVD player 40 reads the rental disc identification information or the sales disc identification information from a DVD mounted by the user, and judges whether the mounted DVD is for rental or for sale, using the read rental disc identification information or the sales disc identification information.

When judging that the DVD is for rental, the DVD player 40 plays back the content in the same manner as that described in the above embodiments.

When judging that the DVD is for sale, the DVD player 40 further reads the media unique information, encrypted content, and encrypted title key from the DVD. Using the read media unique information, the DVD player 40 decrypts the encrypted title key, to generate a title key. The DVD player 40 then decrypts the encrypted content using the generated title key, and plays back the decrypted content.

(8) The following construction is also possible.

The DVD player 40 may internally store a player unique key that is unique to the player.

When the user intends to rent content, the user mounts the IC card 20 onto the DVD player 40. The DVD player 40 writes the player unique key to the IC card 20. Following this, the user ejects the IC card 20 from the DVD player 40, and brings the IC card 20 storing the player unique key to the rental shop.

At the rental shop, the shop clerk mounts the IC card 20 on the shop apparatus 10.

The shop apparatus 10 reads the player unique key from the IC card 20, and encrypts the title key using the read player unique key, and writes the encrypted title key to the IC card 20.

At the time of playing back the content, the DVD player 40 reads the encrypted title key from the IC card 20, and decrypts the read encrypted title key using the internally-stored player unique key, to generate a title key. Following this, the DVD player 40 reads the encrypted content from the DVD 30, decrypts the read encrypted content using the title key, and plays back the decrypted content.

(9) Also, the following modification is possible. The DVD player 40 may internally store a pair of a player private key and a player public key unique to the player. In the same manner as that described above, the DVD player 40 writes the player public key to the IC card 20.

The shop apparatus 10 reads the player public key from the IC card 20, encrypts the title key using the read player public key, and writes the encrypted title key to the IC card 20.

At the time of playing back the content, the DVD player 40 reads the encrypted title key from the IC card 20, and decrypts the read encrypted title key using the internally-stored player private key, to generate a title key. Following this, the DVD player 40 reads the encrypted content from the DVD 30, decrypts the read encrypted content using the title key, and plays back the decrypted content.

(10) Also, the following modification is possible. The DVD player 40 may internally store a player unique key

unique to the player and a player identifier identifying the player.

In the same manner as that described above, the DVD player 40 writes the player identifier to the IC card 20.

The shop apparatus 10 prestores pairs of player identifiers and player unique keys.

The shop apparatus 10 reads the player identifier from the IC card 20, reads the player unique key corresponding to the read player identifier, and encrypts the title key using the read player unique key, and writes the encrypted title key to the IC card 20.

At the time of playing back the content, the DVD player 40 reads the encrypted title key from the IC card 20, and decrypts the read encrypted title key using the internally-stored player unique key, to generate a title key. Following this, the DVD player 40 reads the encrypted content from the DVD 30, decrypts the read encrypted content using the title key, and plays back the decrypted content.

(11) The present invention may also be realized by methods described in the above embodiments. Also, the methods may be realized by computer programs to be executed on a computer, or by digital signals that are made up of the computer programs.

Further, the present invention may be realized by a computer-readable storage medium storing the computer programs or the digital signals. Examples of the

computer-readable recording medium include a flexible disk, a hard disk, a CD-ROM, an MO, a DVD, a DVD-ROM, a DVD-RAM, a BD, and a semiconductor memory. Also, the present invention may be realized by the computer programs, or by the digital signals stored in such a storage medium.

Also, the present invention may be realized by the computer programs or the digital signals being transmitted via an electric communication line, a wireless or cable communication line, or a network such as the Internet.

Moreover, the present invention may be realized by a computer system including a microprocessor and a memory. Here, the memory may store the computer programs, and the microprocessor may operate in accordance with the computer programs.

By storing the computer programs or the digital signals in any of the storage mediums listed above and transferring the storage mediums to an independent computer system, or by transmitting the computer programs or the digital signals to an independent computer system via a network, the computer programs or the digital signals may be executed in the independent computer system.

(12) The above embodiments of the present invention and the modifications may be combined.

Although the present invention has been fully

described by way of examples with reference to the accompanying drawings, it is to be noted that various changes and modifications will be apparent to those skilled in the art. Therefore, unless such changes and modifications depart from the scope of the present invention, they should be construed as being included therein.

Industrial Application

The rental system described above can be used for business purposes i.e., can be used repeatedly and continuously, in the industry where the rental agent rents digitized work, such as music, movies, novels, to the user.